DoD Instruction 4650.08

Positioning, Navigation, and Timing and Navigation Warfare

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective: **Change 1 Effective:**	December 27, 2018 December 30, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at http://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 4650.08, "Positioning, Navigation, and Timing (PNT) and Navigation Warfare (Navwar)," February 5, 2015
Approved by: **Change 1 Approved by:**	Dana S. Deasy, Department of Defense Chief Information Officer Dana S. Deasy, Department of Defense Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance implements positioning, navigation, and timing (PNT) policy pursuant to DoDD 4650.05 and establishes policy, assigns responsibilities, and provides procedures for:

- Integrating PNT and navigation warfare (NAVWAR) across the DoD pursuant to DoDD 4650.05, DoD Instruction (DoDI) 5000.02T, and DoDI 5000.82.
- Ensuring the security of PNT information related to the development, acquisition, sustainment, and operational use of PNT information sources and PNT information-dependent systems pursuant to DoDD 4650.05, DoDI 5000.02T, DoDI 5000.82, and DoDI 8500.01.
- Determining NAVWAR policy compliance and assessing NAVWAR capabilities for programs producing or using PNT information.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

a. The DoD will effectively employ NAVWAR capabilities to ensure a PNT advantage in support of military operations. DoD will use NAVWAR to ensure DoD use of and prevent adversary use of PNT information through coordinated employment of space, cyberspace, and electromagnetic spectrum operations.

b. Programs producing or using PNT information must be NAVWAR-compliant in accordance with this issuance, and will report NAVWAR compliance to the Milestone Decision Authority (MDA) at each acquisition program milestone in accordance with DoDD 5144.02, DoDI 5000.02T, and DoDI 5000.82.

c. NAVWAR compliance effectiveness, including vulnerabilities associated with reliance on a single source of PNT information, will be assessed during plan development for tests, training, exercises, and operations employing PNT information. Section 3 of this issuance describes a compliance process for NAVWAR defensive capabilities (e.g., anti-jam antennas, complementary PNT sources), which must operate in the presence of both friendly and adversary offensive NAVWAR operations (e.g., jamming, cyber threats). All systems that use PNT information, whether or not the system is under Director of Operational Test and Evaluation (DOT&E) oversight, must be tested in and capable of operating in a realistic NAVWAR environment.

d. Reliance on civil, commercial, or foreign sources as the primary means of obtaining PNT information for combat, combat support, or combat service support operations is **not** authorized without a waiver in accordance with CJCS Instruction (CJCSI) 6130.01G. These systems may be utilized as complementary sources, subject to successful NAVWAR compliance determination.

e. Use of civil, commercial, or foreign sources to obtain PNT information for non-combat operations is authorized, subject to successful NAVWAR compliance determination.

f. Weapons or equipment that rely on civil, commercial, or foreign sources as the primary means of obtaining PNT information for combat, combat support, or combat service support operations may not be transferred to a foreign military if a Combatant Command has identified a

NAVWAR interoperability requirement with that foreign military. This restriction is analogous to the restriction on U.S. use of such systems in Paragraph 1.2.d. Even if such a transfer is not prohibited by an interoperability requirement, DoD Components may still prohibit such a transfer, or otherwise mitigate risk, in order to protect the joint force or to minimize civilian casualties (See Paragraphs 2.9.b. and 2.10.b., for DoD Component roles).

g. Through existing information and technology transfer control processes, DoD will ensure a PNT information advantage for U.S. and allied forces.

h. Access to DoD PNT services by U.S. Federal civil agencies and foreign government entities may be authorized in accordance with Paragraph 2.1.e. Access must be approved consistent with applicable U.S. laws, regulations, and DoD policy, including DoD policies for disclosure of classified military information to foreign entities in DoDI 5230.11, and international transfers of technology, articles, and services in DoDI 2040.02.

1.3. SUMMARY OF CHANGE 1.

The changes to this issuance are a result of the establishment of United States Space Command and realignment of responsibilities between United States Space Command and United States Strategic Command. Additionally, in accordance with the August 20, 2019, Director, Defense Technology Security Administration Memorandum, responsibilities for the Director, Defense Security Cooperation Agency, have been added regarding the transfer of weapons or equipment containing civil, commercial, or foreign Global Navigation Satellite System technologies to foreign militaries that have a confirmed NAVWAR interoperability requirement with the United States. Responsibilities for the Director, National Geospatial-Intelligence Agency, have also been added to Section 2. The change also updates references and organizational symbols and makes other administrative changes.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

The DoD CIO:

a. Establishes and implements DoD strategy and policy related to PNT as part of the DoD Information Enterprise in accordance with DoDD 5144.02 and DoDD 3100.10.

b. In accordance with DoDD 4650.05 and DoDI 4650.06, develops and oversees implementation and coordination of PNT and NAVWAR policy through coordinated actions assigned by the DoD PNT Executive Management Board and Oversight Council.

c. Oversees the development and publication of DoD PNT and NAVWAR strategy in support of National Security and military strategy.

d. Assigns responsibilities for determining NAVWAR policy compliance and assessing NAVWAR capabilities for programs producing or using PNT information.

e. Establishes guidance for PNT and NAVWAR support to U.S. Federal agencies and for international cooperation, including policy governing assignment of cryptographic (crypto) networks that support allied and coalition operations, exercises, training, and research and development (R&D) efforts. The DoD CIO coordinates the development of such guidance with the:

(1) Under Secretary of Defense for Policy (USD(P)).

(2) Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)).

(3) Under Secretary of Defense for Intelligence and Security (USD(I&S)).

(4) CJCS.

(5) Secretaries of the Military Departments.

(6) Commander, United States Space Command (CDRUSSPACECOM)

(7) Commander, United States Strategic Command (CDRUSSTRATCOM).

(8) Commander, United States Cyber Command (CDRUSCYBERCOM).

(9) Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

2.2. USD(A&S).

The USD(A&S):

a. Incorporates DoD CIO guidance for PNT and NAVWAR into acquisition and sustainment programs for systems that produce or use PNT information.

b. For programs for which the USD(A&S) is the MDA, oversees acquisition and sustainment-related PNT and system-level architecture issues.

c. Ensures acquisition and sustainment programs are NAVWAR-compliant in accordance with this instruction.

d. Ensures all DoD systems producing or using PNT information are tested in a realistic NAVWAR environment in coordination with the DOT&E and the DoD CIO.

e. In coordination with the DoD CIO, updates acquisition issuances and other supporting guidance as appropriate, to incorporate requirements for determination of NAVWAR compliance at system acquisition decision points.

f. When acting as MDA, determines and confirms NAVWAR compliance at each acquisition milestone for all platforms and systems producing or using PNT information.

2.3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E):

a. Incorporates DoD CIO guidance for PNT and NAVWAR into R&D programs for systems that produce or use PNT information.

b. Reviews test and evaluation plans of acquisition programs for which the USD(A&S) is the MDA to ensure they are sufficient to validate platform or system NAVWAR compliance requirements.

2.4. USD(P).

The USD(P):

a. Provides oversight and guidance to the DoD CIO on international matters as they pertain to this issuance, including oversight and guidance relating to exports and technology transfers of PNT systems and associated technologies.

b. Coordinates with the DoD CIO on items identified in Paragraph 2.1.e.

2.5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS.

In accordance with DoDD 1322.18, the Under Secretary of Defense for Personnel and Readiness provides policy oversight, guidance, and advice on implementing PNT and NAVWAR training in Military Service and joint training.

2.6. DOT&E.

The DOT&E:

a. Coordinates with the USD(A&S) and the DoD CIO to ensure all DoD systems under DOT&E oversight that produce or use PNT information are tested in an operationally realistic NAVWAR environment.

b. For all DoD systems under DOT&E oversight, reviews and approves operational test and evaluation plans to ensure they are adequate to assess PNT and NAVWAR effectiveness, suitability, and survivability.

2.7. DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO).

Under the authority, direction, and control of the USD(I&S), the Director, NRO:

a. Documents NAVWAR electromagnetic warfare support (ES) requirements pursuant to Intelligence Community Directive 115 and CJCSI 5123.01H. Coordinates ES requirements with the CJCS, the Combatant Commanders (CCDRs), the Secretaries of the Military Departments, and the DIRNSA/CHCSS.

b. Provides technical assistance and subject matter expertise to support the Secretaries of the Military Departments as they develop and deploy NAVWAR ES-related capabilities and associated doctrine.

c. For NRO programs fully funded outside of the DoD, considers and documents completion of NRO system-equivalent activities in accordance with Section 3 of this issuance.

2.8. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA).

Under the authority, direction, and control of the USD(I&S), the Director, DIA:

a. Assesses threats to U.S., allied, and coalition PNT and NAVWAR capabilities. Provides intelligence to the CJCS, the CCDRs, and the Secretaries of the Military Departments to support NAVWAR activities. Coordinates with the Military Departments, the Joint Navigation Warfare Center (JNWC), and DOT&E, regarding PNT threat vignettes and scenarios to facilitate exercises, training, and testing.

b. Assesses the vulnerabilities of adversary PNT systems and all adversary equipment that utilizes any type of PNT data or signals, and assesses all adversary offensive NAVWAR capabilities.

c. In coordination with the CJCS, the CCDRs, and the Secretaries of the Military Departments, ensures distribution of threat assessments and intelligence products to U.S. allies and coalition partners, as required to facilitate allied and coalition operations, exercises, and training.

2.9. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA).

Under the authority, direction, and control of the USD(I&S), the Director, NGA:

a. Assesses threats to U.S., allied, and coalition PNT and NAVWAR capabilities.

b. Provides intelligence to the CJCS, the CCDRs, and the Secretaries of the Military Departments to support NAVWAR activities.

c. Coordinates with the Military Departments, the JNWC, and the DOT&E, regarding PNT threat vignettes and scenarios to facilitate exercises, training, and testing.

d. Assesses the vulnerabilities of adversary PNT information systems and NAVWAR capabilities.

e. In coordination with the CJCS, the CCDRs, and the Secretaries of the Military Departments, ensures distribution of threat assessments and intelligence products to U.S. allies and coalition partners, as required to facilitate allied and coalition operations, exercises, and training.

2.10. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S), the DIRNSA/CHCSS:

a. Helps the DoD Components develop and manage PNT information assurance, including cryptography and integrated PNT device design.

b. Provides continuing electronic intelligence analysis of current and evolving systems and associated signals to the DoD Components to ensure correct identification and cataloguing of collected signals.

c. Leads DoD NAVWAR ES cooperative activities with U.S. allies and partners, in coordination with the DoD CIO, the Secretary of the Air Force, and the Director, NRO.

d. Develops a NAVWAR ES implementation plan to support the PNT and NAVWAR strategic plans referenced in Paragraph 2.1.c.

e. Develops procedures to protect PNT information and related cryptography pursuant to DoDD 5230.11 and in coordination with the DoD CIO, the CJCS, and the Secretaries of the Military Departments.

f. Implements allied and coalition partner cryptonet assignments to support allied and coalition operations, exercises, training, and R&D efforts as validated by the CJCS.

2.11. DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY.

Under the authority, direction, and control of the USD(P), the Director, Defense Security Cooperation Agency:

a. Ensures the CCDRs and the Security Cooperation Implementing Agencies receive periodic briefs on policy regarding the transfer of PNT and NAVWAR technology and capability to foreign militaries.

b. Takes actions required to prevent or mitigate transfer, via Foreign Military Sales, of weapons or equipment identified in Paragraph 1.2.f.

2.12. DIRECTOR, DEFENSE TECHNOLOGY SEUCURITY ADMINISTRATION.

Under the authority, direction, and control of the USD(P), the Director, Defense Technology Security Administration, takes actions required to prevent or mitigate transfer, via direct commercial sales, of weapons or equipment identified in Paragraph 1.2.f. and in accordance with DoDI 2040.02.

2.13. SECRETARIES OF THE MILITARY DEPARTMENTS

The Secretaries of the Military Departments:

a. When an official acting under the authority, direction, and control of the Secretary of a Military Department is serving as MDA or other acquisition decision authority, ensure the MDA or decision authority, as appropriate, determines and confirms NAVWAR compliance at each acquisition decision point for all platforms and systems producing or using PNT information, in accordance with DoDI 5000.02T, DoDI 5000.82, and Section 3 of this issuance.

b. When an official acting under the authority, direction, and control of the Secretary of a Military Department is serving as MDA, ensure that the MDA reviews test and evaluation plans to ensure they are sufficient to validate platform or system NAVWAR compliance requirements.

c. Identify PNT contributions and NAVWAR environment assumptions, including all intentional and unintentional electromagnetic interference (including both Red and Blue electromagnetic attack elements), and ensure they are addressed in applicable Military Service

concepts, plans, and doctrine pursuant to and in accordance with this instruction. Coordinate with the other Military Departments, the JNWC, the NGA, and the DIA, regarding PNT threat vignettes and scenarios to facilitate exercises, training, and testing. Collaborate with United States Space Command and United States Strategic Command in the application of standardized NAVWAR threat conditions outlined in the PNT biennial assessment in determining relevant NAVWAR environments.

d. Designate a representative from each of their respective Military Departments to identify and advocate for PNT and NAVWAR requirements to establish and formalize joint NAVWAR requirements in accordance with CJCSI 3170.01H.

e. Conduct tests, training, and exercises in an operationally realistic NAVWAR environment with validated concepts of operation. Evaluate U.S., allied, and coalition NAVWAR capabilities versus assessed PNT and NAVWAR capabilities of potential adversaries.

f. Provide requirements to the Director, DIA, and the Director, NGA, for assessment of:

(1) Vulnerabilities of U.S., allied, and coalition PNT systems and receivers and adversary offensive NAVWAR capabilities that threaten them.

(2) Vulnerabilities of adversary PNT information systems and NAVWAR capabilities.

g. Develop procedures to safeguard keyable PNT devices throughout their life cycle, including procedures for the destruction of security-controlled PNT devices, in coordination with the CJCS and the DIRNSA/CHCSS.

h. Ensure Security Classification Guides for all programs producing or using PNT information protect the specific PNT technologies and integration methods used.

i. Ensure all systems or platforms producing or using PNT information incorporate an open architecture design for the integration of multiple PNT sources to the maximum extent practicable in accordance with the Modular Open Systems Approach guidance contained in DoDI 5000.02T and in Section 805 of Public Law 114-328. PNT subsystems, if not designated as major system components, should have the attributes ascribed to major system components, as defined by Section 805 of Public Law 114-328 due to the need to address evolving technologies and threats.

j. Report to the DoD CIO the Service MDA determination regarding NAVWAR compliance for each platform or system under consideration for development or production following each acquisition milestone decision.

2.14. CJCS.

The CJCS:

a. Ensures PNT and NAVWAR assumptions and considerations are addressed in joint concepts, plans, and doctrine pursuant to and in accordance with this instruction.

b. Ensures joint tests, training, and exercises are conducted in an operationally realistic NAVWAR environment.

c. Oversees allied and coalition partner crypto network assignment in support of allied and coalition operations, exercises, training, and R&D efforts in coordination with the DIRNSA/CHCSS.

d. Coordinates and formalizes joint PNT and NAVWAR requirements and capabilities across the DoD in accordance with CJCSI 5123.01H.

e. Ensures all requirements documents for systems and platforms producing or using PNT include the system survivability key performance parameter (KPP), as described in Paragraph 3.2.a.

2.15. CDRUSSPACECOM.

The CDRUSSPACECOM:

a. Coordinates Global Positioning System (GPS)/PNT- and NAVWAR-related tests, training, and exercises and events with the appropriate Defense and Federal departments and agencies to:

(1) Develop a process to coordinate and prioritize GPS and NAVWAR testing in the National Airspace System.

(2) Prioritize and de-conflict overlapping GPS and NAVWAR testing and training events in the National Airspace System.

(3) Ensure impacts to GPS users outside the boundaries of the testing, training, and exercise/event areas are minimized.

b. Exercises command authority regarding the operational control of DoD space-based PNT assets.

c. Advocates for joint resilient PNT requirements and capabilities supporting NAVWAR operations for the DoD.

d. Supports Combatant Command joint training and planning related to NAVWAR operations; provides contingency joint resilient PNT and NAVWAR planning and operations for

other Combatant Commands; and maintains the JNWC as the center of excellence for NAVWAR.

e. Conducts allied and coalition partner GPS cryptonet assignments in support of allied and coalition operations, exercises, training, and R&D efforts in coordination with the DIRNSA/CHCSS.

f. As the Joint Proponent for PNT and NAVWAR operations, integrates and coordinates PNT and NAVWAR capabilities across the DoD and provides a biennial assessment of PNT and NAVWAR operational capabilities to the DoD CIO.

g. Conducts PNT operational field assessments of DoD, adversary, and coalition NAVWAR capabilities and vulnerabilities to identify capability gaps, assess operational risk, and gain knowledge to enable PNT superiority in joint force and combined operations.

h. In conjunction with the Secretaries of the Military Departments and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, provides requirements to the Director, DIA, and the Director, NGA, for assessment of:

(1) Vulnerabilities of U.S., allied, and coalition PNT systems and receivers and adversary offensive NAVWAR capabilities that threaten them.

(2) Vulnerabilities of adversary PNT information systems and blue offensive NAVWAR capabilities to threaten them.

i. Collaborates with the Military Services, United States Special Operations Command, and other Combatant Commands in the application of standardized NAVWAR threat conditions outlined in the biennial DoD PNT assessment in determining relevant condition levels to enable evaluation and testing of PNT capabilities.

j. Supports the United States Northern Command in assessing PNT- and NAVWAR-related threat effects to U.S. critical infrastructure.

2.16. CDRUSSTRATCOM.

The CDRUSSTRATCOM provides support regarding employment and advocacy of PNT capabilities affecting nuclear command, control, and communications mission areas for which USSTRATCOM is responsible and regarding use of electromagnetic spectrum in support of NAVWAR.

2.17. CDRUSCYBERCOM.

The CDRUSCYBERCOM:

a. Advocates for PNT and NAVWAR capabilities to support Department of Defense Information Network operations.

b. Ensures the necessary actions are taken to secure and defend Department of Defense Information Network operations that could be impacted by any hostile or malicious attack against a Department of Defense Information Network PNT asset.

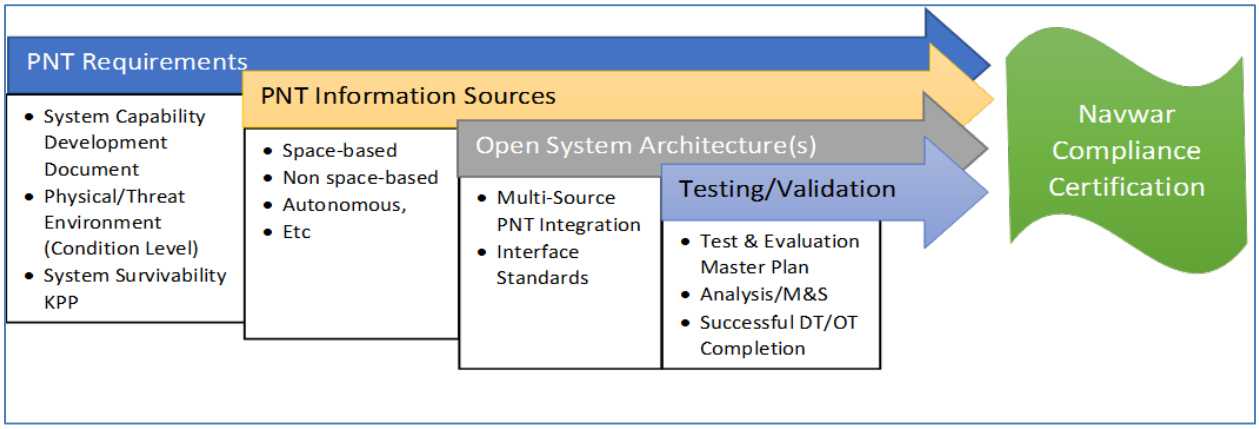
c. In coordination with CDRUSSPACECOM, and other Combatant Commanders as required, ensures cyber capabilities are developed, realistically tested, and made available in support of Joint Force NAVWAR mission needs.

SECTION 3: NAVWAR COMPLIANCE PROCEDURES

3.1. DISCUSSION.

The purpose of the following NAVWAR compliance procedures is to prescribe clearly the steps that must be taken for any program or system that uses PNT information to determine successfully whether they are NAVWAR compliant. A system is NAVWAR compliant if it continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment. Figure 1 provides a pictorial view of the components of the NAVWAR compliance process.

Figure 1. NAVWAR Compliance Process Components



3.2. CAPABILITY DEVELOPMENT AND SYSTEM INTEGRATION.

a. Each program or system producing or using PNT information must incorporate the following system survivability KPP in its capability development document: The PNT capabilities employed by the program or system must maintain tactical resiliency and continue to provide trusted PNT information at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment for a minimum of "x" period of time (the "x" being the period of time the platform or system needs accurate PNT to successfully complete its mission in this expected NAVWAR environment).

b. Each program or system will determine the worst-case NAVWAR environment within which the platform or system will be required to operate. Table 1 may be used as a model for this determination. Condition levels should be described in sufficient detail to enable evaluation and testing of PNT capabilities planned for use by DoD platforms or systems to operate successfully and demonstrate tactical resiliency within required NAVWAR and physical environments. These condition levels should be used in conjunction with standardized threat levels during the development and operational testing processes, ranging from low to high threat levels.

c. Each program or system producing or using PNT information must determine what mix of PNT capabilities, integrated using a Modular Open System Approach to the maximum extent possible, is necessary to meet the system survivability KPP defined in the capability development document in the worst-case environment.

Table 1. Notional PNT Conditions and Capabilities for NAVWAR Compliance

Level	Condition	PNT Capability
0	**Low** - mission accomplished without precision PNT	**No Special PNT Protection** - Commercial GPS Standard Positioning Service (SPS) without authentication, unkeyed military GPS receivers in SPS mode, any GNSS Open Service signals, or other PNT sources not previously considered and accepted for use by the DoD
1	**Moderate** - mission accomplished at slightly degraded level (slower pace, reduced weapon selection, some collateral damage) without precision PNT	**Limited PNT Access** - Keyed P(Y) and M-Code equipment, other trusted signals (with authentication), or accepted signals of opportunity which may be available
2	**High** - mission accomplished at degraded level (slower pace, limited selection of precision weapons, collateral damage, fratricide) without precision PNT	**Assured PNT in Challenged Environments** - Keyed M-Code or P(Y)-Code receivers with self-contained PNT source(s), authorized foreign GNSS through Memorandum of Agreement with DoD, or approved terrestrial RF navigation signals
3	**Extremely High** - mission accomplished at an extremely degraded level (very slow pace, no use of precision weapons, imminent danger of collateral damage/ fratricide) without precision PNT	**Assured PNT in Severe Environments** - Keyed GPS M-Code or P(Y)-Code receivers [assumes use of assistive technology and AJ augmentations] or self-contained PNT source(s) operating within its/their effective performance envelope(s)

3.3. DEVELOPMENTAL AND OPERATIONAL TEST AND EVALUATION.

a. Review system test and evaluation plans for programs producing or using PNT information to ensure they are sufficient to validate platform or system NAVWAR compliance assessment. The USD(R&E) will conduct the review of test and evaluation plans of acquisition programs for which the USD(A&S) is the MDA, and the responsible Service authority will conduct the review of test and evaluation plans of acquisition programs for which the MDA is at the Service level.

b. Conduct system test and evaluation (e.g., real-world test; modeling and simulation; empirical analysis) sufficient to validate that all systems or platforms producing or using PNT information meet the system survivability KPP referred to in Paragraph 3.2.a.

3.4. MODIFICATION OF FIELDED PNT CAPABILITIES AND AQUISITIONS OUTSIDE THE DEFENSE ACQUISITION SYSTEM.

Any platform or system undergoing PNT capability modification or upgrade, or acquired outside the Defense Acquisition System, is subject to Paragraphs 1.2.c., 1.2.d., and 1.2.e. Capability developers and DoD Components must consider and demonstrate to the responsible Service authority completion of equivalent activities to those described in Paragraphs 3.2. and 3.3. to ensure NAVWAR compliance. The Component Acquisition Executive or DoD Component chief information officer must notify the DoD PNT Executive Management Board of NAVWAR compliance. The notification template is contained in DoDM O-4650.11. The notification must address the requirements of either Paragraph 1.2.d. or 1.2.e. in the following manner:

a. Combat, Combat Support, and Combat Service Support.

The system is NAVWAR compliant if the PNT capabilities employed by the program or system are capable of providing trusted PNT information over the time periods and at the level of accuracy required for all missions in which it is used in the expected physical, electromagnetic, and cyber environment.

b. Non-Combat Operations.

In the event the PNT capability incorporates civil, commercial, or foreign sources, the system is NAVWAR compliant if the PNT capability provides trusted PNT information over the time periods and at the level of accuracy required for all missions in which it is used in the expected physical, electromagnetic, and cyber environment.

GLOSSARY

G.1. ACRONYMS.

CCDR	Combatant Commander
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSPACECOM	Commander, United States Space Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
crypto	cryptographic
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoT&E	Director of Operational Test and Evaluation
ES	electromagnetic warfare support
GPS	Global Positioning System
JNWC	Joint Navigation Warfare Center
KPP	key performance parameter
MDA	Milestone Decision Authority
NAVWAR	navigation warfare
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
PNT	positioning, navigation, and timing
R&D	research and development
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary for Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purposes of this issuance.

TERM	DEFINITION
combat service support	Defined in the DoD Dictionary of Military and Associated Terms.
combat support	Defined in the DoD Dictionary of Military and Associated Terms.
ES	Defined in the DoD Dictionary of Military and Associated Terms.
integrated PNT	A combination of multiple PNT sources, NAVWAR, and joint and Service doctrine meant to provide assured PNT information to military users operating in a NAVWAR environment.
NAVWAR	Defined in the DoD Dictionary of Military and Associated Terms.
NAVWAR compliance	A PNT system that continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment.
NAVWAR environment	The expected physical, electromagnetic, and cyber conditions in which a PNT system operates.
NAVWAR interoperability requirement	Established when a Combatant Command identifies a country's need for GPS cryptography to enable military interoperability per Chairman of the Joint Chiefs of Staff Instruction 6510.06C.
strategic plan	A strategy that aligns requirements with timelines for specific materiel and non-materiel solutions to provide a means to establish priorities and forecast technology developments, as well as a framework to coordinate efforts.
trusted PNT information	PNT information that can be continuously verified or validated.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 5123.01H, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," August 31, 2018

Chairman of the Joint Chiefs of Staff Instruction 6130.01G, "Master Positioning, Navigation, and Timing Plan," June 3, 2019 [1]

Chairman of the Joint Chiefs of Staff Instruction 6510.06C, "Communication Security Releases to Foreign Nations," November 8, 2013[1]

Director, Defense Technology Security Administration Memorandum, "Prohibiting the Use of Precision Guided Munitions equipped with Global Positioning System Standard Positioning Service," August 20, 2019

DoD Directive 1322.18, "Military Training," January 13, 2009 as amended

DoD Directive 3100.10, "Space Policy," October 18, 2012, as amended

DoD Directive 4650.05, "Positioning, Navigation, and Timing (PNT)," June 9, 2016, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 4650.06, "Positioning, Navigation, and Timing Management," June 16, 2016

DoD Instruction 5000.2T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

DoD Instruction 5000.82, "Acquisition of Information Technology," April 21, 2020

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Manual O-4650.11, "Positioning, Navigation, and Timing (PNT) Security," May 26, 2017, as amended

Intelligence Community Directive 115, "Intelligence Community Capability Requirements Process," December 21, 2012

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Public Law 114–328, Section 805, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016

1 Releasability is limited (not approved for public release). This instruction is approved for .mil/.gov access only onthe Non-classified Internet Protocol Router Network (NIPRNet). DoD Components) and otherFederal agencies may obtain copies of this issuance through controlled access at https://sso.jsp.osd.mil/adfs/ls. DoD Components may also obtain access on the Secret Internet Protocol Router Network (SIPRNet) Directives Electronic Library Website.